

Information Security Policy

Siemens considers itself the trusted partner and leader in industrial cybersecurity resilience that brings the most added value to our customers, partners, society and ourselves in the digital and real world by providing industry-leading solutions that meet engineering best practices in the various sectors where it operates.



Information Security Objectives

Siemens recognizes the importance of ensuring the protection of the information entrusted to it, both for the market and for customers and employees, and to this end its main objectives are:

- Align information security with the organizational strategy and business objectives, protecting data and systems cohesively.
- Strive for the protection of the confidentiality, integrity, and availability of information under our responsibility.
- Work towards implementing protective measures for Information Technology and Operational Technology (IT/OT) facilities and systems through continuous risk assessment.
- Develop and refine an efficient information security incident management process to enable rapid response, minimize impacts, and support business continuity.
- Foster a culture of information security, raising awareness among employees and partners about their responsibilities and providing the necessary resources for security management.
- Collaborate with relevant organizations, government agencies, and associations to enhance information security globally.

Commitments

Siemens, through its top management, is guided by internationally recognized best practices and is committed to the following:

- Actively engaging in developing and continuously enhancing an effective Information Security Management System (ISMS), encompassing policies, standards, and processes aimed at safeguarding our services and information assets against relevant threats.
- Being dedicated to advancing our continuous risk management framework to thoroughly assess threats and vulnerabilities and progressing diligently with the implementation of controls designed to mitigate risks to acceptable levels.
- Establishing mechanisms for periodic reviews of the ISMS by the Steering Committee, with the aim of continually improving its suitability, effectiveness, and overall enhancement.
- Diligently pursuing adherence to all applicable normative, legal, regulatory, and contractual requirements, as well as information security guidelines.
- Focusing on optimizing the allocation of necessary resources and actively developing comprehensive programs to cultivate appropriate training and awareness for all employees, thereby nurturing a robust security culture.
- Being dedicated to championing the authenticity of information and actively working to integrate ethical considerations and sustainable practices into all cybersecurity initiatives.

Sofia Tenreiro
Siemens SA Chief Executive Officer

Ricardo Nunes
Siemens SA Chief Financial Officer

Paula Monteiro
Siemens SA Cybersecurity Officer



Visit our website for more information about Siemens AG's Cybersecurity Governance:
Lisboa, Maio 2026

Unrestricted